CLAIMS

1. A system for producing multiple-symbol randomizer sequences over GF(2^m), the system including:

A. a first register for supplying an initial state, the register holding a non-zero element of GF(2^m);

B. a first multiplier for multiplying the contents of the register by a multiplier constant that is a primitive element of GF(2^m); and

C. first feedback means for

i. supplying the products produced by the multiplier as the symbols of the randomizer sequence, and

ii. supplying the symbols of the randomizer sequence to update the first register.

2. The system of claim 1 further including:

D. one or more second registers for holding elements of GF(2^m);

E. one or more second multipliers for multiplying the contents of the one or more second registers by one or more multiplier constants that are elements of GF(2^m);

F. an adder for adding the products produced by the first and second multipliers and supplying the sum to the first feedback means; and

G. second feedback means to supplying the contents of the first register to update the second register.

3. The system of claim 1 further including a selection means for selecting the initial state of the first register in order to produce a randomizer sequence that provides for encryption.

4. The system of claim 2 further including a selection means a means for selecting an initial state for the first register and the one or more second registers.

5. The system of claim 1 further including encryption means for encrypting a code word, the encryption means including:

a. selection means for selecting an initial state for use in producing the randomizer sequence;

b. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, the means producing a randomized code word; and

c. means for producing a key associated with the selected the initial state.

6. The system of claim 5 further including a decrypting subsystem for using the key to reproduce the randomizer sequence and removing the randomizer sequence from the randomized code word to reproduce the ECC code word.

7. The system of claim 1 wherein the multiplier constant is selected to produce randomizer sequences that are each a predetermined minimum distance from code words of a given BCH code.

8. The system of claim 6 further including means for detecting mis-synchronization, the mis-synchronization detection means including:

a. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, the means producing a randomized code word;

b. means for removing the randomizer sequence from the randomized code word to reproduce the ECC code word; and

c. a decoder for decoding the reproduced ECC code word, the decoder detecting a mis-synchronization if the number of errors in the reproduced ECC code word is greater than the number of errors that can be corrected by the given BCH code.

9. The system of claim 7 wherein the multiplier constant is further selected from a set of multiplier constants which each produce randomizer sequences that are at least a predetermined minimum distance from code words of a given BCH code.

10. The system of claim 9 further including a means for providing a key to select the multiplier constant for a given randomizer sequence.

11. The system of claim 2 wherein the multiplier constants are selected to produce randomizer sequences that are each a predetermined minimum distance from code words of a given BCH code.

12. The system of claim 11 further including means for detecting mis-synchronization, the mis-synchronization detection means including:

a. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, the means producing a randomized code word;

b. means for removing the randomizer sequence from the randomized code word to reproduce the ECC code word; and

c. a decoder for decoding the reproduced ECC code word, the decoder detecting a mis-synchronization if the number of errors in the reproduced ECC code word is greater than the number of errors that can be corrected by the given BCH code.

13. The system of claim 12 wherein the multiplier constants are further selected from a set of multiplier constants that produce randomizer sequences that are at least a predetermined minimum distance from code words of a given BCH code.

14. The system of claim 13 further including a means for providing a key to select the multiplier constants for a given the randomizer sequence.

15. The system of claim 1 further including

D. one or more second registers for holding elements of $GF(2^m)$;

E. one or more second multipliers for multiplying the contents of the first register by associated elements of $GF(2^m)$ and supplying the products to update the one or more second registers; and

F. one or more adders for adding the contents of the one or more second registers to the product produced by the first multiplier to produce a sum and supplying the sum to the first feedback means.

16. The system of claim 1 further including:

D. a plurality of second multipliers each for multiplying the contents of the register by a multiplier constant that is a primitive element of $GF(2^m)$; and

E. a switch for selecting one of the plurality of second multipliers or the first multiplier to produce the randomizer sequence.

17. The system of claim 16 further including encryption means for encrypting a code word, the encryption means including:

d. selection means for selecting an initial state for use in producing the randomizer sequence;

e. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, the means producing a randomized code word; and

f. means for producing a key associated with the selected the initial state.

18. The system of claim 17 further including decryption means for using the key to reproduce the randomizer sequence and removing the randomizer sequence from the randomized code word to reproduce the ECC code word.

19. The system of claim 18 wherein the selection means further selects the multiplier constant from a set of multiplier constants.

20. The system of claim 15 further including encryption means for encrypting a code word, the encryption means including:

g. selection means for selecting an initial state for use in producing the randomizer sequence;

h. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, the means producing a randomized code word; and

i. means for producing a key associated with the selected the initial state.

21. The system of claim 20 further including decryption means for using the key to reproduce the randomizer sequence and removing the randomizer sequence from the randomized code word to reproduce the ECC code word.

22. The system of claim 20 wherein the selection means further selects the multiplier constant from a set of multiplier constants.

23. A method for producing multiple-symbol randomizer sequences, the method including the steps of:

A. supplying an initial state to a first register;

B. producing a first product by multiplying the contents of the first register by a multiplier constant that is a primitive element of $GF(2^m)$;

C. supplying the first product as

a. a next symbol of the randomizer sequence, and

b. an to update the first register;

D. repeating steps A-C i times for $i \leq 2^m-2$.

24. The method of claim 23 further including:

E.. in the step of supplying the initial state further including supplying an initial state to a second register;

F. in the step of producing a first product further including multiplying the contents of the second register by a multiplier constant that is an element of $GF(2^m)$ and adding the result to the first product; and

G. in the step of supplying the first product further including supplying the contents of the second register to update the first register.

25. The method of claim 23 further including the step of selecting the initial state for the first register in order to produce a randomizer sequence for encryption.

26. The method of claim 25 further including, in the step of selecting the initial state, selecting the initial state of the second register.

27. The method of claim 26 further including the step of associating with each randomizer sequence a key that indicates the associated selected initial state.

28. The method of claim 23 further including in the step of producing the fist product further including selecting the multiplier constant to produce randomizer sequences that are each a predetermined minimum distance from code words of a given BCH code.

29. The method of claim 28 further including the step of detecting mis-synchronization by

a. combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, to produce a randomized code word;

b. removing the randomizer sequence from the randomized code word to reproduce the ECC code word; and

c. decoding the reproduced ECC code word and detecting a mis-synchronization if the number of errors in the reproduced ECC code word is greater than the number of errors that can be corrected by the given BCH code.

30. The method of claim 28 wherein in the step of producing the first product further includes selecting the multiplier constant from a plurality of multiplier constants which each produce randomizer sequences that are respectively a predetermined minimum distance from code words of a given BCH code.

31. The method of claim 30 further including the step of providing a key to select the multiplier constants associated with a given randomizer sequence.

Sub a1

32. The method of claim 23 further including

E. in the step of supplying the initial state supplying the initial state of one or more second registers;

F. in the step of producing the first product including the step of multiplying the contents of the first register in one or more second multipliers by associated primitive elements of $GF(2^m)$ and supplying the products to update the one or more second registers; and

G. in the step supplying further including the step of adding the contents of the one or more second registers to the product associated with the contents of the first register and supplying the sum as the next sequence symbol and to update the first register.

33. The method of claim 23 further including in the step of producing the first product selecting a multiplier constant from a plurality of multiplier constants.

34. The method of claim 23 further including a step of encrypting a code word by:

j. selecting an initial state for use in producing the randomizer sequence;

k. combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$ to produce a randomized code word; and

l. producing a key associated with the selected the initial state.

35. The method of claim 34 further including a step of decrypting the code word by using the key to reproduce the randomizer sequence and removing the randomizer sequence from the randomized code word to reproduce the ECC code word.

36. The method of claim 34 wherein the step of selecting the initial state further includes selecting one or more multiplier constants.